TRƯỜNG ĐẠI HỌC HỒNG ĐỨC
KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

THUYẾT MINH

ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN
NĂM HỌC 2022-2023

NGHIÊN CỨU ỨNG DỤNG CÁC KỸ THUẬT PHÂN LỚP DỮ LIỆU NHẰM PHÁT HIỆN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDOS)

Thuộc nhóm ngành khoa học: Khoa học máy tính

THANH HÓA, THÁNG 09/2022

TRƯỜNG ĐẠI HỌC HỒNG ĐỨC

KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

THUYẾT MINH

ĐỀ TÀI NGHIÊN CỨU KHOA HỌC CỦA SINH VIÊN NĂM HỌC 2022-2023

NGHIÊN CỨU ỨNG DỤNG CÁC KỸ THUẬT PHÂN LỚP DỮ LIỆU NHẰM PHÁT HIỆN HÌNH THỨC TẤN CÔNG TỪ CHỐI DỊCH VỤ PHÂN TÁN (DDOS)

Thuộc nhóm ngành khoa học: Khoa học máy tính

Nhóm sinh viên thực hiện(đại diện): Lê Xuân Quang
Giới tính: Nam
Dân tộc: Kinh
Lớp, khoa: K23A, CNTT&TT Năm thứ: 3 /Số năm đào tạo: 4
Ngành học: Công nghệ thông tin

Người hướng dẫn: TS. Nguyễn Thế Cường

THANH HÓA, THÁNG 09/2022

TRƯỜNG ĐẠI HỌC HỒNG ĐỨC
KHOA CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

THUYẾT MINH ĐỀ TÀI
NGHIÊN CỨU KHOA HỌC SINH VIÊN
Năm học 2022 - 2023

1. Tên đề tài: Nghiên cứu ứng dụng các kỹ thuật phân lớp dữ liệu nhằm phát hiện hình thức tấn công từ chối dịch vụ phân tán (DDoS).

2. Cấp dự thi

Cấp trường.

3. Nhóm sinh viên thực hiện

3.1. Họ và tên(người đại diện): Lê Xuân Quang
Lớp: K23A-CNTT Khoa: Công nghệ thông tin
Điện thoại: 0852747537 Email: lexuanquang1408@gmail.com
3.2. Họ và tên: Lê Đình Thắng
Lớp: K23A-CNTT Khoa: Công nghệ thông tin
Điện thoại: 0925058118 Email: ledinhthang.thvn@gmail.com
3.3. Họ và tên: Cao Sơn Đăng
Lớp: K23A-CNTT Khoa: Công nghệ thông tin
Điện thoại: 0367756372 Email: dangkudo230202@gmail.com
3.4. Họ và tên: Hoàng Văn Huy
Lớp: K23A-CNTT Khoa: Công nghệ thông tin
Điện thoại: 0859734136 Email: Hoangvanhuy1709@gmail.com

4. Cơ quan chủ trì

Khoa Công nghệ thông tin và Truyền thông.

5. Lĩnh vực nghiên cứu

Công nghệ thông tin.

6. Loại hình nghiên cứu

Triển khai.

7. Thời gian thực hiện

8 tháng, từ tháng 09/2022 đến 04/2023.

8. Sự cần thiết của đề tài

Theo các báo cáo của securelist.com, trên toàn cầu, quý 1 năm 2022 đã phát hiện 91.052 cuộc tấn công DDoS. Hầu hết các cuộc tấn công (94,95%) kéo dài dưới 4 giờ, nhưng cuộc tấn công dài nhất tiếp tục trong 549 giờ (gần 23 ngày)[1].Trong quý 2 năm 2022, phát hiện 78558 cuộc tấn công. Hoạt động tăng đều đặn trong suốt quý: trung bình từ 731 cuộc tấn công mỗi ngày vào tháng 4 lên 845 vào tháng 5, lên 1195 vào tháng 6[2].

Đặc biệt, các thông báo được đăng ngày 21/8/2022 thì Google vừa chặn đứng cuộc tấn công DDoS lớn nhất từ trước tới nay, với đỉnh điểm lên tới 46 triệu yêu cầu

mỗi giây (rps), lớn hơn 76% so với đợt tấn công kỷ lục từng được ghi nhận trước đó. Theo bài đăng, quy mô của cuộc tấn công tương đương với việc hứng chịu toàn bộ lượng truy cập trong 1 ngày của Wikipedia - một trong những trang web có lưu lượng truy cập lớn nhất thế giới - chỉ trong vòng 10 giây[3].

Theo dữ liệu từ Cục An ninh mạng, Bộ công an, trong 6 tháng đầu năm 2021 đã phát hiện 2.551 vụ tấn công mạng, 5,4 triệu lượt địa chỉ IP của các cơ quan Nhà nước bị tấn công với 15 biến thể mã độc. Có gần 250 báo, tạp chí điện tử trong tổng số hơn 800 cơ quan báo chí. Đáng chú ý là các cơ quan truyền thông, báo chí luôn nằm trong top bị tấn công từ chối dịch vụ (DDoS). Việt Nam đứng thứ 6 về nguồn tấn công DDoS trên toàn cầu, sau Trung Quốc, Mỹ, Pháp, Nga và Brazil. Trong khi đó, tại khu vực châu Á - Thái Bình Dương, Việt Nam đứng thứ 2 về nguồn tấn công DDoS[4].

Các số liệu thống kê cho thấy tổn thất về kinh tế, dữ liệu, tài nguyên… mà DDoS gây ra rất lớn. Cùng với sự phát triển của trí thông minh nhân tạo, chúng tôi quyết định chọn đề tài: "**Nghiên cứu ứng dụng các kỹ thuật phân lớp dữ liệu nhằm phát hiện hình thức tấn công từ chối dịch vụ phân tán (DDoS)**" nhằm đóng góp một phần nhỏ vào công cuộc an ninh mạng.

[1] securelist.com, (2022) "DDoS attacks in Q1 2022".

[2] securelist.com, (2022) "DDoS attacks in Q2 2022".

[3] vov.vn, (2022) "Google chặn cuộc tấn công DDoS lớn nhất từ trước đến nay".

[4] mic.gov.vn, (2022) "Tìm giải pháp an toàn cho hệ thống thông tin trọng yếu".

9. Sơ lược về tình hình nghiên cứu trong và ngoài nước về vấn đề chọn nghiên cứu

a. Tình hình nghiên cứa trong nước

Tại Việt Nam đã có nhiều nghiên cứu về tấn công từ chối dịch vụ phân tán(DDoS) và cách ngăn chặn[5]. Cũng đã có nghiên cứu về các kỹ thuật phân lớp dữ liệu, khai phá dữ liệu. Các nghiên cứu tại Việt Nam mới chỉ nghiên cứu các mảng riêng lẻ như quản lý khách hàng[6], dự báo… Vẫn chưa chú trọng nghiên cứu về phân lớp dữ liệu nhằm phát hiện tấn công từ chối dịch vụ phân tán(DDoS).

[5] Hoàng Tuấn Ngọc, (2017) "Nghiên cứu tấn công DDoS và xây dựng giải pháp ngăn chặn".

[6] Trương Tiến Dưỡng, (2020) "Nghiên cứu ứng dụng phân lớp dữ liệu trong quản lý khách hàng trên mạng".

b. Tình hình nghiên cứu ngoài nước

Trên thế giới cũng có nhiều nghiên cứu, phân tích về tấn công từ chối dịch vụ phân tán cũng như phân lớp dữ liệu như:

Các kỹ thuật mới để gây ra các cuộc tấn công DDoS và giảm thiểu các cuộc tấn công này được chứng minh rõ ràng là hoạt động tốt hơn nhiều so với các kỹ thuật hiện có[7].

Trong khi đó, có nhiều nghiên cứu về phân lớp dữ liệu dựa vào các phương pháp

như SVM, cây quyết định[8]…

[7] KS Vanitha; SV UMA; SK Mahidhar,(2018) “Distributed denial of service: Attack techniques and mitigation”.

[8] opSonali Agarwal, G. N. Pandey, and M. D. Tiwari, (2019) “Data Mining in Education: Data Classification and Decision Tree Approach”.

10. Mục tiêu nghiên cứu

Hiểu được nguyên lý hoạt động của hình thức tấn công mạng DDoS. Hiểu rõ các phương pháp phân lớp dữ liệu. Căn cứ vào các đặc điểm của hình thức tấn công đề xuất được giải pháp nhận dạng các hình thức tấn công DDoS và đưa ra được giải pháp khắc phục khi bị tấn công DDoS.

11. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu

Các phương pháp tấn công DDoS và các giải pháp nhận dạng tấn công DDoS.

Phạm vi nghiên cứu

Dữ liệu về các tấn công dạng DDoS trong mạng các dịch vụ.

12. Nội dung nghiên cứu

- Nghiên cứu cơ sở lý thuyết về hình thức tấn công từ chối dịch vụ DDoS.
- Nghiên cứu các phương pháp phân lớp dữ liệu.
- Nghiên cứu về một số kĩ thuật dùng để dự đoán, nhận diện hình thức tấn công DDoS.
- Nghiên cứu cơ sở dữ liệu mẫu về hình thức tấn công DDoS đã có.
- Xây dựng mô hình dùng đề phát hiện hình thức tấn công DDoS dựa vào dữ liệu mẫu đã có.
- Đánh giá hiệu quả của mô hình.

13. Phương pháp nghiên cứu

- Phương pháp phân tích và tổng hợp lý thuyết: Nghiên cứu các tài liệu, các báo cáo khoa học, các luận văn, luận án liên quan đến lĩnh vực khai phá dữ liệu; nghiên cứu các tài liệu mô tả về dữ liệu hiện có liên quan đến hình thức tấn công DDoS.

- Phương pháp thực nghiệm: xây dựng thử nghiệm các mô hình dự đoán; đánh giá kết quả của các mô hình đã có, mô hình đề xuất; phân tích, tổng hợp kết quả.

14. Hiệu quả và phạm vi sử dụng (kinh tế, xã hội, giáo dục, khoa học, kỹ thuật,..) và tính mới, đóng góp mới của đề tài

Tạo mô hình tối ưu nhằm phát hiện tấn công DDoS, đóng góp ứng dụng cho cộng đồng.

15. Dự kiến kết quả

- Tổng quan cơ sở lý thuyết về an ninh mạng, các phương pháp phân lớp dữ liệu và hình thức tấn công DDoS.
- Phân tích, đánh giá được dữ liệu về các cuộc tấn công DDoS đã có.

- Xây dựng được mô hình dự đoán, phát hiện được các tấn công DDoS.
- Đánh giá được mô hình phát hiện tấn công DDoS dựa vào thông tin liên quan.

16. Nội dung và tiến độ thực hiện công việc

TT	Nội dung công việc	Kết quả cần đạt được	Thời gian		Người thực hiện	Ghi chú
			Bắt đầu	Kết thúc		
1	Xây dựng và bảo vệ thuyết minh đề tài	Thuyết minh đề tài	09/2022	10/2022	Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn Huy	
2	Tìm hiểu mô hình để nhận diện đối tượng, các phương pháp tối ưu mô hình	Tài liệu tìm hiểu	10/2022	12/2022	Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn Huy	
3	Nghiên cứu xây dựng mô hình	Các giải pháp đề xuất và chương trình thực nghiệm	12/2022	04/2023	Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn Huy	
4	Tổng hợp, viết báo cáo, viết bài báo khoa học, nghiệm thu đề tài	Đề tài được xếp loại Khá trở lên.	04/2022	04/2023	Lê Đình Thắng, Lê Xuân Quang, Cao Sơn Đăng, Hoàng Văn Huy	

17. Sản phẩm

Mô hình dự đoán, phát hiện được các tấn công DDoS.

18. Nhu cầu kinh phí để thực hiện đề tài:

Theo quy chế chi tiêu nội bộ (Ban hành theo Quyết định 2443/QĐ-ĐHHĐ ngày 25 tháng 10 năm 2022 của Hiệu trưởng trường Đại học Hồng Đức) - Kinh phí đề tài dự thi cấp trường, cấp khoa: 2.000.000 đ/đề tài.

19. Đề xuất các yêu cầu, điều kiện cho thực hiện đề tài

Thanh Hóa, ngày 10 tháng 09 năm 2022

KT.Hiệu trưởng **Phó Hiệu trưởng**	**Đơn vị chủ trì**	**GV hướng dẫn**	**Trưởng nhóm**
Hoàng Thị Mai	**Phạm Thế Anh**	**Nguyễn Thế Cường**	**Lê Xuân Quang**